



CVE-2020-5243

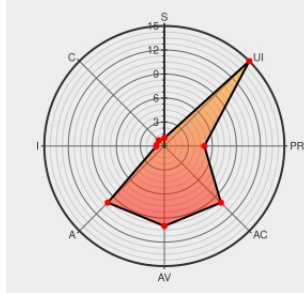
Published on: 02/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-5243 - advisory for GHSA-cmcx-xhr8-3w9p

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H



Certain versions of [Uap-core](#) from [Uap-core Project](#) contain the following vulnerability:

uap-core before 0.7.3 is vulnerable to a denial of service attack when processing crafted User-Agent strings. Some regexes are vulnerable to regular expression denial of service (REDoS) due to overlapping capture groups. This allows remote attackers to overload a server by setting the User-Agent header in an HTTP(S) request to maliciously crafted long strings. This has been patched in uap-core 0.7.3.

CVE-2020-5243 has been assigned by [GitHub](#) security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [ua-parser](#) - [uap-core](#) version < 0.7.3

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Denial of Service in uap-core <=0.7.2 when processing crafted User-Agent strings · Advisory · ua-parser/uap-core · GitHub

Exploit

Third Party Advisory

github.com

text/html

CONFIRM

github.com/ua-parser/uap-core/security/advisories/GHSA-cmcx-xhr8-3w9p

Merge pull request from GHSA-cmcx-xhr8-3w9p · ua-parser/uap-core@0afd61e · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/ua-parser/uap-core/commit/0afd61ed85396a3b5316f18bfd1edfaadf8e88e1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

983117 Nodejs (npm) Security Update for uap-core (GHSA-cmcx-xhr8-3w9p)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Uap-core Project	Uap-core	All	All	All	All
Application	Uap-core Project	Uap-core	All	All	All	All
cpe:2.3:a:uap-core_project:uap-core:*****:.*						
cpe:2.3:a:uap-core_project:uap-core:*****:.*						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →